Theoretical Computer Science 9 (1979) 147–150

NOTE

A COUNTEREXAMPLE TO A CONJECTURE OF SCHNORR REFERRING TO MONOTONE NETWORKS

Ingo WEGENER
Fakultät für Mathematik, Universität Bielefeld 4800 Bielefeld 1, F.R.G.

Communicated by M.S. Paterson
Received September 1978
Revised December 1978

Abstract. Schnorr [1] proved a lower bound on the number of additions in monotone computations of rational polynomials. He conjectured a similar lower bound on the number of $\vee$-gates in monotone networks computing monotone Boolean functions. We disprove this conjecture.

Let Ω_+^b be the set of all monotone Boolean functions that means all functions $f:\{0,1\}^n \to \{0,1\}$ ($n \in \mathbf{N}$) which may be computed by networks if only $\wedge$- and $\vee$-gates are available. $C_{\wedge,\vee}(f)$ is the minimal number of $\wedge$- and $\vee$-gates in any monotone network computing f. Schnorr [1] considered a different complexity measure: $C_\vee(f)$, the minimal number of $\vee$-gates ($\wedge$-gates have cost zero) in any monotone network computing f. Obviously $C_\vee(f) \leq C_{\wedge,\vee}(f)$. Therefore one is interested in proving lower bounds on $C_\vee(f)$.

We introduce some well known definitions. Let $x_1, \ldots, x_n$ be Boolean variables. A monom t is a product of variables: $t(x_1, \ldots, x_n) = \bigwedge_{i \in S} x_i$, $S \subset \{1, \ldots, n\}$. A monom t is an implicant of $f \in \Omega_+^b$ iff $t \leq f$ ($t = 1$ implies $f = 1$). An implicant t of f is a prime implicant of f iff no monom $t' > t$ is an implicant of f (no shortening of a prime implicant is still an implicant). Let $\mathrm{PI}(f)$ be the set of all prime implicants of f. It is well known that $f(x_1, \ldots, x_n) = \bigvee_{t \in \mathrm{PI}(f)} t(x_1, \ldots, x_n)$. This representation is called the monotone disjunctive normal form of f (MDNF).

Definition 1. $B \subset \mathrm{PI}(f)$ is b-separated iff

$$\forall r \in \mathrm{PI}(f)\ \forall s, t \in B: \quad r \geq s \wedge t \Rightarrow (r = s \text{ or } r = t).$$

Definition 2. $\#_b(f) := \max\{|B| - 1 \mid B \subset \mathrm{PI}(f), B \text{ } b\text{-separated}\}$.

Schnorr [1] stated the following conjecture:

$$\forall f \in \Omega_+^b: \quad C_\vee(f) \geq \#_b(f). \tag{1}$$

In the case of the monotone computation of a monotone rational polynomial f we substitute "$\cdot$" for "$\wedge$", "+" for "$\vee$" and rational variables for Boolean variables.

Besides this all positive rational numbers are possible entries of the network. Let $L_+(f)$ be the minimal number of additions in each monotone computation of f and let $\#(f)$ be a complexity measure for f based on a similar definition of separateness as stated in Definition 1 and 2. Schnorr [1] proved for all monotone rational polynomials f: $L_+(f) \geq \#(f)$. Therefore one may suppose that the conjecture (1) is valid too.

We disprove this conjecture. In [2] the author investigated the monotone complexity of functions which are generalizations of the Boolean matrix product. One got a good lower bound for the necessary number of $\wedge$-gates but not for the necessary number of $\vee$-gates. On the contrary an astonishing small upper bound for the number of $\vee$-gates was proved. The functions g_M which are defined below are based on these functions.

g_M will be a function of M^3+6M variables which will be labelled x^i_{hl} ($1 \leq i \leq 3$, $1 \leq h \leq M$, $1 \leq l \leq 2$) and $y_{h_1h_2h_3}$ ($1 \leq h_1, h_2, h_3 \leq M$).

Definition 3. We define $g_M \in \Omega^b_+$ by its MDNF:

$$g_M := g_M(x^1_{11}, \ldots, x^3_{M2}, y_{111}, \ldots, y_{MMM})$$
$$:= \bigvee_{1 \leq h_1, h_2, h_3 \leq M, 1 \leq l \leq 2} y_{h_1h_2h_3} x^1_{h_1l} x^2_{h_2l} x^3_{h_3l}.$$

Lemma 1. $C_\vee(g_M) \leq M^3+6M^2+3M-1$.

Proof. Let

$$z_{h_1h_2h_3} := x^1_{h_11} x^2_{h_21} x^3_{h_31} \vee x^1_{h_12} x^2_{h_22} x^3_{h_32}.$$

(The functions $z_{h_1h_2h_3}$ all together form the function f^3_{M2} which has been investigated in [2].) We can rewrite

$$g_M = \bigvee_{1 \leq h_1, h_2, h_3 \leq M} y_{h_1h_2h_3} \wedge z_{h_1h_2h_3}.$$

Now we define a monotone network computing g_M.

Step 1. Compute for all $i, j \in \{1, 2, 3\}$ and all $h_1, h_2, h_3 \in \{1, \ldots, M\}$

$$a^{ij}_{h_ih_j} := x^i_{h_i1} \vee x^j_{h_j2}.$$

If $i = j$ we have M possibilities to choose (h_i, h_j). If $i \neq j$ we have M^2 possibilities to choose (h_i, h_j). Therefore Step 1 requires $6M^2+3M$ $\vee$-gates (and no $\wedge$-gate).

Step 2. Compute for all $i \in \{1, 2, 3\}$ and all $h_1, h_2, h_3 \in \{1, \ldots, M\}$

$$b^i_{h_1h_2h_3} := (a^{i1}_{h_ih_1} \wedge a^{i2}_{h_ih_2}) \wedge a^{i3}_{h_ih_3} = x^i_{h_i1} \vee x^1_{h_12} x^2_{h_22} x^3_{h_32}.$$

Step 2 requires no $\vee$-gate (but $3M^2+3M^3$ $\wedge$-gates). (If Step 2 is used in a

computation of a rational polynomial we obtain the term $(x^i_{h_i 1})^3$ and other undesired terms.)

Step 3. Compute for all $h_1, h_2, h_3 \in \{1, \ldots, M\}$

$$c_{h_1h_2h_3} := b^1_{h_1h_2h_3} \wedge b^2_{h_1h_2h_3} \wedge b^3_{h_1h_2h_3}$$
$$= x^1_{h_11} x^2_{h_21} x^3_{h_31} \vee x^1_{h_12} x^2_{h_22} x^3_{h_32} = z_{h_1h_2h_3}.$$

Step 3 requires no $\vee$-gate (but $2M^3$ $\wedge$-gates). (Steps 1, 2 and 3 compute all $z_{h_1h_2h_3}$ by its monotone conjunctive normal form.)

Step 4. Compute for all $h_1, h_2, h_3 \in \{1, \ldots, M\}$

$$d_{h_1h_2h_3} := y_{h_1h_2h_3} \wedge c_{h_1h_2h_3} = y_{h_1h_2h_3} \wedge z_{h_1h_2h_3}.$$

Step 4 requires no $\vee$-gate (but M^3 $\wedge$-gates).

Step 5. Compute

$$g_M = \bigvee_{1 \le h_1, h_2, h_3 \le M} d_{h_1h_2h_3}.$$

Step 5 requires $M^3 - 1$ $\vee$-gates (and no $\wedge$-gate).

Combining the results of all five steps we have proved the lemma.

Remark: Our network requires $6M^3 + 3M^2$ $\wedge$-gates.

Lemma 2. $\mathrm{PI}(g_m)$ *is b-separated.*

Proof. Let $r, s, t \in \mathrm{PI}(g_M)$ and $r \geqslant s \wedge t$. We have to prove $r = s$ or $r = t$. We may write $r = y_{h_1h_2h_3} x^1_{h_1l} x^2_{h_2l} x^3_{h_3l}$:

$$s = y_{h_1'h_2'h_3'} x^1_{h_1'l'} x^2_{h_2'l'} x^3_{h_3'l'} \quad \text{and} \quad t = y_{h_1''h_2''h_3''} x^1_{h_1''l''} x^2_{h_2''l''} x^3_{h_3''l''}.$$

For each monom m let $V(m)$ be the set of all variables which are contained in m. Since $r \geqslant s \wedge t$: $V(r) \subset V(s) \cup V(t)$.

Without loss of generality we may assume $y_{h_1h_2h_3} = y_{h_1'h_2'h_3'}$.

Case 1. $l = l'$. Obviously $r = s$.

Case 2. $l \neq l'$. Therefore $x^i_{h_il} \neq x^i_{h_il'}$ for all $i \in \{1, 2, 3\}$. Since $V(r) \subset V(s) \cup V(t)$ we conclude for all i $x^i_{h_il} = x^i_{h_il''}$. In particular $h_i = h_i''$ for all i and therefore $y_{h_1h_2h_3} = y_{h_1''h_2''h_3''}$. All together we have proved $r = t$.

Lemma 3. $\#_b(g_M) = 2M^3 - 1$.

Proof. $\mathrm{PI}(g_M)$ is b-separated (Lemma 2) and $\mathrm{PI}(g_M)$ is the largest possible b-separated set (Definition 1). Therefore (by Definition 2) $\#_b(g_M) = |\mathrm{PI}(g_M)| - 1 = 2M^3 - 1$ where the last equality follows from the definition of g_M.

Fact 1. $\forall M \geq 7$: $M^3+6M^2+3M-1<2M^3-1$.

By Lemma 1, Lemma 3 and Fact 1 we have proved the following theorem:

Theorem. $\forall M \geq 7$: $C_\vee(g_M) < \#_b(g_M)$.

Therefore the conjecture (1) is disproved.

Remark. Our network contains $6M^3+3M^2$ $\wedge$-gates and M^3+6M^2+3M-1 $\vee$-gates, that means $7M^3+9M^2+3M-1$ gates on the whole. Obviously this network is not optimal. We need only $2M^2+2M^3$ $\wedge$-gates to compute all $(x^1_{h_1 l} \wedge h^2_{h_2 l}) \wedge x^3_{h_3 l}$. Afterwards M^3 $\vee$-gates are sufficient to compute all $z_{h_1 h_2 h_3}$. Finally we take M^3 $\wedge$-gates and M^3-1 $\vee$-gates to compute

$$g_M = \bigvee_{1 \leq h_1, h_2, h_3 \leq M} y_{h_1 h_2 h_3} \wedge z_{h_1 h_2 h_3}.$$

This network contains only $5M^3+2M^2-1$ gates.

Also some modifications of Schnorr's conjecture remain open:

(1) every optimal monotone network for f requires $\#_b(f)$ $\vee$-gates

(2) $C_{\wedge,\vee}(f) \geq \#_b(f)$.

References

[1] C.P. Schnorr, A lower bound on the number of additions in monotone computations, *Theoret. Comput. Sci.* **2** (1976) 305–315.

[2] I. Wegener, Switching functions whose monotone complexity is nearly quadratic, *Theoret. Comput. Sci.* **9** (1) (1979) 83–97.